UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/656,166	09/06/2000	Brad Kollmyer	PM PM271173	8916

23552	7590	03/09/2004

MERCHANT & GOULD PC
P.O. BOX 2903
MINNEAPOLIS, MN 55402-0903

EXAMINER
NALVEN, ANDREW L

ART UNIT	PAPER NUMBER
2134	10

DATE MAILED: 03/09/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

	Application No.	Applicant(s)
	09/656,166	KOLLMYER ET AL.
Office Action Summary	Examiner	Art Unit
	Andrew L Nalven	2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM
THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *06 September 2003*.

2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-99* is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-99* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *06 September 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All   b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.

4)☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.

5)☐ Notice of Informal Patent Application (PTO-152)

6)☐ Other: _____.

DETAILED ACTION

1.   Claims 1-99 are pending.

2.   Amendment received on 12/2/03 has been entered and considered.

Claim Objections

3.   Claims 47 and 52 are objected to because of the following informalities:

4.   Claims 47 and 52 recite the same limitations and are dependent from the same

parent claim. Appropriate correction is required.

Claim Rejections - 35 USC § 112

5.   The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly
> claiming the subject matter which the applicant regards as his invention.

6.   Claims 11, 63, 77, and 80 are rejected under 35 U.S.C. 112, second paragraph,

as being indefinite for failing to particularly point out and distinctly claim the subject

matter which applicant regards as the invention.

7.   Claim 11 contains a limitation citing a determination as to "the correctness of a

result." The limitation is vague and indefinite as it is unclear what the "result" pertains

to.

8.   Claims 63, 77, and 81 cite a limitation stating, "Negotiating and exchanging of the

key is carried out during the streaming session." Claims 63, 77, and 80 depend from

claims 62, 76, and 80 respectively that state the limitation "negotiator negotiates and

exchanges a key before the combined data is transmitted over the network." The cited

limitations appear to contradict each other. Appropriate correction and clarification is

required.

Claim Rejections - 35 USC § 102

9.   The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that

form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

10.   Claims 1-14, 16-21, 23-25, 29-30, 36, 39-40, 42, 48-50, 53-57, 61-63, 65-70, 73-

81, 84-89 and 94-97 are rejected under 35 U.S.C. 102(b) as being anticipated by

Wasilewski US Patent No 5,420,866. Wasilewski teaches a system for providing

conditional access information to decoders in a packet based multiplexed

communications system.

11.   With regards to claims 1, 25, 53, 61, 67, 69, 73 and 78-79, Wasilewski teaches a

parser configured to parse a first portion of the data from a second portion (Wasilewski,

column 9 lines 30-36, Figure 1), an encrypter configured to encrypt the first portion of

the data (Wasilewski, column 9 lines 30-36), and a combiner configured to combine the

encrypted first portion of the data with the second portion of the data wherein the

second portion of the data includes more than routing information (Wasilewski, column 9 lines 30-36, Figure 1, Figure 3B).

12.   With regards to claims 2 and 88, Wasilewski teaches data including streaming data (Wasilewski, column 7 line 64 – column 8 line 6).

13.   With regards to claims 3, 30, and 42, Wasilewski teaches the first portion of the data including payload data (Wasilewski, column 9 lines 30-31).

14.   With regards to claims 4, 29, 54, 65, 68, 75, 85, and 89, Wasilewski teaches the second portion of the data containing header and control data (Wasilewski, column 9 lines 34-36 and 51-62).

15.   With regards to claims 5 and 6, Wasilewski teaches a transmitter for configured to send the combined first and second portions of the data over the network to the client (Wasilewski, Figure 2) and a receiver configured to receive the data from the server before the data is sent over the network to the client (Wasilewski, Figure 2).

16.   With regards to claim 7, Wasilewski teaches a device configured to establish a data stream between the server and the client (Wasilewski, column 8 lines 22-30).

17.   With regards to claims 8, 20, 39, and 95, Wasilewski teaches a key negotiator configured to negotiate an encryption key with the client (Wasilewski, column 9 lines 37-58).

18.   With regards to claims 9, 40, 56-57, 62-63, 76-77, 80-81, 94 and 96, Wasilewski further teaches key negotiation and key exchange occurring during transmission of a stream (Wasilewski, column 9 lines 37-58).

19.   With regards to claim 10, Wasilewski teaches the encrypter being transparent to the server (Wasilewski, column 7 line 64 – column 8 line 13).

20.   With regards to claim 11 (as best understood), Wasilewski teaches key negotiation determining the correctness of a result (Wasilewski, column 13 lines 45-49, column 14 line 62 – column 15 line 6).

21.   With regards to claim 12, Wasilewski teaches a decrypter configured to decrypt the first portion of the data (Wasilewski, column 13 lines 41-49 and column 14 lines 21-25).

22.   With regards to claim 13, Wasilewski teaches the parser being configured to parse the data into different portions based on the media format (Wasilewski, column 13 line 50 – column 14 line 4).

23.   With regards to claim 14, Wasilewski teaches the encrypter being configured to encrypt the first portion of data based on the media format (Wasilewski, column 9 lines 51-54 and column 8 lines 37-40).

24.   With regards to claim 16, Wasilewski teaches an implementation on an encryption bridge (Wasilewski, Figure 2 Item 11).

25.   With regards to claim 17, Wasilewski teaches the parsing of received data into portions including a first portion and second portion (Wasilewski, column 9 lines 30-36, Figure 1), encrypting the first portion of the data (Wasilewski, column 9 lines 30-36), and sending the received data including the encrypted first portion and the second portion over the network to the client (Wasilewski, column 8 lines 17-21 and Figure 2).

26.   With regards to claims 18 and 66, Wasilewski teaches the data source being a server (Wasilewski, Figure 2).

27.   With regards to claim 19, Wasilewski teaches the determination of whether a stream is established between the server and client (Wasilewski, column 13 lines 39-49, column 14 line 62 – column 15 line 6).

28.   With regards to claim 21, Wasilewski teaches received data being streaming data (Wasilewski, column 7 line 64 – column 8 line 6) and key negotiation carried out during the streaming session (Wasilewski, column 9 lines 37-58).

29.   With regards to claim 23, Wasilewski teaches the encryption key being negotiated with a decryption shim on the client (Wasilewski, column 9 lines 37-58, Figure 2 Item 206, Figure 6 Items 138 and 140).

30.   With regards to claim 24, Wasilewski teaches the step of determining whether received data is streaming data (Wasilewski, column 13 lines 50-63).

31.   With regards to claims 36 and 86, Wasilewski teaches a client receiving data over a network (Wasilewski, column 13 lines 35-39 and Figure 2), parsing the data into portions including a first and second portion (Wasilewski, column 13 line 50 – column 14 line 9), decrypting the first portion of the data (Wasilewski, column 14 lines 21-44), and passing the decrypted first portion of the data to a higher level of operations for play in the client (Wasilewski, column 15 lines 6-17 and Figure 6).

32.   With regards to claim 48, Wasilewski teaches the payload data including multimedia data (Wasilewski, column 8 lines 52-57).

33.   With regards to claims 49 and 50, Wasilewski teaches the parser being

configured to parse the data into different portions based on the data protocol used to

transmit (Wasilewski, column 8 lines 31-35).

34.   With regards to claim 55, Wasilewski teaches streaming data included in the at

least one data portion to remain unencrypted (Wasilewski, column 9 lines 19-36).

35.   With regards to claim 70, Wasilewski teaches the portion of the data to be

encrypted includes media data encoded in a media format (Wasilewski, column 7 line

50 – column 8 line 21) and the encoder encrypts based on the media format

(Wasilewski, column 14 lines 9-13).

36.   With regards to claims 74 and 84, Wasilewski teaches the downloaded data

being included in the encrypted portion of the data (Wasilewski, column 8 lines 6-17).

37.   With regards to claim 87, Wasilewski teaches the encrypted portion of the

transmitted data including media data (Wasilewski, column 8 lines 52-57), and the data

transmitter being configured to send the decrypted media to the media player resident

on the client (Wasilewski, Figures 2 and 6).

38.   With regards to claim 97, Wasilewski teaches the determining of a plurality of

portions of data (Wasilewski, column 9 lines 30-36, Figure 1), selectively encrypting at

least one portion of the plurality of portions (Wasilewski, column 9 lines 30-36),

authenticating a client to receive the selectively encrypted portion (Wasilewski, column

14 line 62 – column 15 line 6), and transmitting the selectively encrypted portion to the

authenticated client (Wasilewski, column 8 lines 17-21 and Figure 2).

Claim Rejections - 35 USC § 103

39.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set
> forth in section 102 of this title, if the differences between the subject matter sought to be patented and
> the prior art are such that the subject matter as a whole would have been obvious at the time the
> invention was made to a person having ordinary skill in the art to which said subject matter pertains.
> Patentability shall not be negatived by the manner in which the invention was made.

40.   Claims 15, 26-28, 31-35, 37-38, 43-47, 52, 64, 71-72, 82-83, 90-93, and 99 are

rejected under 35 U.S.C. 103(a) as being unpatentable over Wasilewski US Patent No

5,420,866 in view of Graunke et al US Patent No 5,991,399.

41.   With regards to claims 15 and 71, Wasilewski as described above teaches a

system where encryption algorithms may be changed (Wasilewski, column 9 lines 15-

19) but fails to teach a pluggable core encoding an encryption algorithm. Graunke

teaches a pluggable core for a decoding algorithm (Graunke, column 7 lines 40-46). At

the time the invention was made, it would have been obvious to a person of ordinary

skill in the art to utilize the ideas of Graunke's pluggable decoding core to fashion an

encoding core because it offers the advantage of helping prevent a malicious user from

learning the algorithm or key by making the key easily changeable (Graunke, column 4

line 63 – column 5 line 51).

42.   With regards to claims 26-27, Wasilewski as modified fails to teach the

determining if a shim is present or the downloading of the shim. Graunke teaches the

determining if a shim is present or the downloading of the shim (Graunke, column 4

lines 45-50). At the time the invention was made, it would have been obvious to a

person of ordinary skill in the art to utilize Graunke's method of downloading the shim

because it offers the advantage of allowing cryptography to be dynamic by changing

keys and methods thus increasing protection of digital content (Graunke, column 2 line

59 – column 3 line 3).

43.   With regards to claim 28, Wasilewski as modified fails to teach the determining of

whether an encryption key is current. Graunke teaches a determination as to whether

the encryption key is current (Graunke, column 9 lines 7-15). At the time the invention

was made, it would have been obvious to a person of ordinary skill in the art to use

Graunke's method of checking if a key is current because it offers the advantage of

allowing a system to use dynamically generated keys that change for different content

thus increasing security and preventing a situation where a single stolen key may

unlock all available content (Graunke, column 2 lines 52-67).

44.   With regards to claims 31 and 43, Wasilewski as modified fails to teach the

determining if a packet is the last packet in the data stream. Graunke teaches the

determining if a packet is the last packet in the data stream (Graunke, column 9 lines

15-16).

45.   With regards to claims 32 and 44, Wasilewski as modified teaches the use of a

decryption shim but fails to teach receiving feedback from a decryption shim if it is

determined that the packet is not the last packet in the stream. Graunke teaches the

determination that a packet is not the last packet in the stream (Graunke, Figure 4B

'134').

46.   With regards to claims 33-35, 45-47, 52, 64, 82 and 90-93, Wasilewski as

modified teaches a streaming session, but fails to teach examining means to determine

if the client has been comprised. Graunke teaches examining means to terminate

communication if the client has been compromised (Graunke, column 8 lines 33-60). At

the time the invention was made, it would have been obvious to a person of ordinary

skill in the art to utilize Graunke's disclosed examining means because it offers the

advantage of helping prevent malicious users or code from modifying software in order

to gain unauthorized access to digital content (Graunke, column 1 lines 14-44).

47.   With regards to claims 37-38, Wasilewski as modified teaches the determining if

a stream is unencrypted and the passing of the decrypted data to a higher level of

operation (Graunke, column 4 lines 37-40). At the time the invention was made, it

would have been obvious to a person of ordinary skill in the art to utilize Graunke's

method of passing unencrypted data to a higher level of operation because it allows the

user to view the contents of the media (Graunke, column 2 lines 38-43).

48.   With regards to claim 72, Wasilewski as modified teaches an implementation on

an encryption bridge (Wasilewski, Figure 2 Item 11).

49.   With regards to claim 83, Wasilewski as modified teaches the second portion of

the data containing header and control data (Wasilewski, column 9 lines 34-36 and 51-

62).

50.   With regards to claim 99, Wasilewski as modified teaches the client transmitting

a self-generated certificate (Graunke, column 8 lines 12-18, column 7 lines 10-15).

51.   Claims 22, 41, 51, 58-59 are rejected under 35 U.S.C. 103(a) as being

unpatentable over Wasilewski US Patent No 5,420,866 in view of Graunke et al US

Patent No 5,991,399 and further in view of Dorfman et al US Patent No 6,449,651.

52.   With regards to claims 22, 41 and 58, Wasilewski as described above fails to

teach the examining of the client during the streaming session and terminating the

streaming session if the encryption key is invalid. Graunke teaches examining means

to terminate communication if the client has been compromised (Graunke, column 8

lines 33-60) and Dorfman teaches a determination if a key is invalid (Dorfman, column 7

line 53 – column 8 line 11). At the time the invention was made, it would have been

obvious to a person of ordinary skill in the art to utilize Graunke's method of termination

if a client is compromised and Dorfman's method of determining if a key is invalid

because Graunke offers advantage of helping prevent malicious users or code from

modifying software in order to gain unauthorized access to digital content (Graunke,

column 1 lines 14-44), while Dorfman offers the advantages of ensuring that a key is not

used beyond the expiration date (Dorfman, column 2 lines 55-65) and increasing

security by ensuring a key has not been tampered with (Dorfman, column 3 lines 1-42).

53.   With regards to claim 51, Wasilewski as modified teaches a feedback signal to

stop transmission (Graunke, column 8 lines 57-60).

54.   With regards to claim 59, Wasilewski as modified teaches the data source being

a server (Wasilewski, column 8 lines 22-30), examining carried out on an encryption

bridge between the server and the network (Wasilewski, Figure 2 Item 11), so

encrypting and combining is transparent to the server (Wasilewski, column 7 line 64 –

column 8 line 13).

55.   With regards to claim 60, Wasilewski as modified teaches key negotiating and

exchanging and the decryption using the key is carried out using a shim on the client

(Wasilewski, column 9 lines 37-58, Figure 2 Item 206, Figure 6 Items 138 and 140) and

the shim is configured so that negotiating and exchanging is transparent to the client

(Wasilewski, Figure 2 Item 206).

56.   Claim 98 is rejected under 35 U.S.C. 103(a) as being unpatentable over

Wasilewski US Patent No 5,420,866 in view of Fawcett et al US Patent No 5,678,002.

Wasilewski, as described above, the accepting of a shim from a server that is

selectively encrypting a portion of data (Wasilewski, column 9 lines 30-36, column 9

lines 37-58, Figure 2 Item 206, Figure 6 Items 138 and 140), but fails to teach a

confirmation sent back from the shim. Fawcett teaches a confirmation sent back from a

software module after accepting the module (Fawcett, column 8 lines 1-13). At the time

the invention was made, it would have been obvious to a person of ordinary skill in the

art to utilize Fawcett's method of sending confirmations because it offers the advantage

of informing the server that a successful download is complete so further processing

may then take place (Fawcett, column 8 lines 7-13).

Conclusion

57.   The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

58.   Markham US Patent No 5,796,836 teaches a scalable key agile cryptography system.

59.   Pebley et al US Patent No 6,154,840 teaches a system and method for transferring encrypted sections of documents across a computer network.

60.   Pinder et al US Patent No 6,424,717 teaches encryption devices for use in a conditional access system.

61.   Any inquiry concerning this communication or earlier communications from the examiner should be directed to Andrew L Nalven whose telephone number is 703 305 8407. The examiner can normally be reached on Monday - Thursday 8-6, Alternate Fridays.

   If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached on 703 308 4789. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the

Patent Application Information Retrieval (PAIR) system. Status information for

published applications may be obtained from either Private PAIR or Public PAIR.

Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should

you have questions on access to the Private PAIR system, contact the Electronic

Business Center (EBC) at 866-217-9197 (toll-free).

Andrew Nalyen
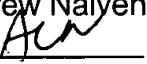
MATTHEW SMITHERS
PRIMARY EXAMINER
Art Unit 2137